WESTMINSTER SCHOOL

DATA PROTECTION POLICY

Author: Andrew Thorpe-Apps
Lead: Bursar and Chief Operating Officer

Reviewer: Audit, Risk and Compliance Committee

Shared Policy across Westminster Great School and Westminster Under School

Date: October 2024
Review Date: May 2027

WESTMINSTER SCHOOL

DATA PROTECTION POLICY

INTRODUCTION

Data protection is an important legal and regulatory compliance issue for Westminster School. The School's approach to data protection not only seeks to ensure the welfare and safety of its pupils and staff, but also the security and efficient running of the School. The School will protect and maintain a balance between data protection rights in accordance with the UK General Data Protection Regulation (GDPR). This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, workers and other third parties.

For the avoidance of doubt, references in this policy to "Westminster School" and "School" include both Westminster Great School (WGS) and Westminster Under School (WUS). Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations. All staff, governors and contractors are required to familiarise themselves with this policy and comply with the provisions contained in it.

During the course of the School's activities it collects, stores and processes personal data, and sometimes sensitive data known as "Special Category Data" about staff, pupils, their parents, its governors, contractors and other third parties in a manner more fully detailed in the School's Privacy Notices. The School, as "data controller", is liable for the actions of its staff and governors in how they handle data. It is therefore an area where all staff and governors have a part to play in ensuring they comply with their legal obligations, whether that personal data handling is sensitive or routine.

CONTEXT

The law changed on Friday, 25 May 2018 with the implementation of the General Data Protection Regulation (GDPR) – an EU Regulation that continues to be directly effective in the UK – and the enactment of the Data Protection Act 2018 (DPA 2018) to deal with certain issues left for national law. The DPA 2018 includes specific provisions of relevance to independent schools: in particular, in the context of our safeguarding obligations, and regarding the right of access to personal data.

Following the end of the Brexit transition period on 31 December 2020, the GDPR was retained in UK law as the UK GDPR, and continues to be read alongside the DPA 2018, with technical amendments to ensure it can function in UK law.

The Information Commissioner's Office (ICO) is responsible for enforcing data protection law and will typically look into individuals' complaints routinely and without cost. The ICO has various powers to take action for breaches of the law, including the option to fine an entity up to £17.5 million or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher.

The School's registration under the DPA 2018 is: Z2553168. The school's registration details are available online from the ICO website and at the School by appointment.

DEFINITIONS
Key data protection terms used in this policy are as follows:

Automated Processing
Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. An example of automated processing includes profiling and automated decision making. Automatic decision-making is when a decision is made which is based solely on automated processing (without human intervention) which produces legal effects or significantly affects an individual. Automated decision-making is prohibited except in exceptional circumstances.

Data Controller
Person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the School (including its governors) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller.

Data Processor
An entity that processes personal data on behalf of a data controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.

Data Protection Impact Assessment (DPIA)
This a process to help the School identify and minimise the data protection risks of a project. The School must do a DPIA for processing anything that is likely to result in a high risk to individuals.

Data Protection Officer (DPO)
The DPO assists the School in monitoring internal compliance, informing and advising the School in its data protection obligations, and providing advice regarding DPIAs. The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.

Data Subject
An identified or identifiable living individual to whom personal data relates.

Personal Data Breach
A breach of security or human error leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Personal information (or "personal data")
Any information relating to a Data Subject by which that individual may be identified, that is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings, school

reports, photographs, medical information etc.). The definition includes expressions of opinion about the individual or any indication of the School's, or any person's, intentions towards that individual.

Processing
Virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, updating it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it. Processing begins when a Data Controller starts making a record of information about a Data Subject, and continues until the Data Controller no longer needs the information and it has been securely destroyed. Note that holding personal information on someone counts as processing even if nothing else is done with it.

Special Category Data
This includes personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences. This form of personal data requires more protection because it is sensitive.

APPLICATION OF THIS POLICY

This policy sets out the School's expectations and procedures with respect to processing any personal data that might be collected from Data Subjects (including parents, pupils, employees, governors, contractors and third parties).

Those who handle personal data as employees or governors of the School are obliged to comply with this policy when doing so. For employees, breaches of this policy may result in disciplinary action. Accidental breaches of the law or this policy in handling personal data will happen from time to time, for example by human error, and will generally be treated as a disciplinary issue. However, failure to report breaches that pose significant risks to the School or individuals will be considered a serious matter and most likely result in disciplinary action.

In addition, this policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether they are acting as "Data Processors" on the School's behalf (in which case they will be subject to binding contractual terms) or as Data Controllers responsible for handling such personal data in their own right.

Where the School shares personal data with third party Data Controllers – which may range from other schools, to parents, to appropriate authorities, to casual workers and volunteers – each party will need a lawful basis to process that personal data, and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy.

Volunteers or contractors are Data Controllers in their own right, but the same legal regime and best practice standards set out in this policy will apply to them by law.

PERSONS RESPONSIBLE FOR DATA PROTECTION

The School has appointed as the Head of Legal, Risk and Assurance to oversee all data protection for matters relating to pupils and staff. The Head of Legal, Risk and Assurance reports directly to the Bursar and Chief Operating Officer.

The Head of Legal, Risk and Assurance will endeavour to ensure that all personal data is processed in compliance with this policy, the Records Retention Policy, and the principles of the DPA 2018. They are responsible for ensuring that:

- Any Data Subject Rights, including Subject Access Requests, are responded to appropriately within statutory timeframes.
- Checking and approving third parties that handle the School's data.
- Ensuring that the School's policies and data protection framework is kept up to date.
- Arranging data protection training.
- Providing advice and guidance to staff and the Governing Body.
- Keeping the Governing Body, SMC (WGS) and SMT (WUS) updated about data protection responsibilities, risks and any other relevant issues.

The Director of Digital Strategy and Operations is responsible for:

- Ensuring all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services that the School uses to store or process data.

Together the Bursar and Chief Operating Officer; Head of Legal, Risk and Assurance; and, Director of Digital Strategy and Operations form the Data Protection Team and can be contacted should there be any queries or concerns regarding personal data by email: dataprotection@westminster.org.uk.

All staff, governors and contractors involved with the collection, processing and disclosure of personal data must adhere to the following principles:

- Staff should only ever share information on a "need to know basis"; seniority does not give an automatic right to information.
- Data protection should never be used as an excuse for not sharing information where necessary. The welfare of the child is paramount.
- Records of any sort (and particularly email), could at some point in the future be disclosed, whether as a result of litigation or investigation, or because of a subject access request under the DPA 2018. Therefore, when recording information, accuracy, clarity and objectivity should be paramount.
- Personal data should be retained only as long as is necessary, in line with the Records Retention Policy and Retention Schedules, and destroyed securely.
- No member of staff is permitted to remove Special Category Data from School premises, whether in paper or electronic form with two exceptions:
    - The School's pupil database and staff email may be accessed on personal devices provided that the device is secure and Multi Factor Authentication (MFA) protected.
    - For pupils on residential trips, medical information and other relevant information (e.g.: passport details) may be taken off site by the trip leader.

THE PRINCIPLES
The GDPR sets out six principles relating to the processing of personal data which must be adhered to by Data Controllers (and Data Processors). These require that personal data must be:

1. Processed **lawfully, fairly** and in a **transparent** manner;
2. Collected for **specific and explicit purposes** and only for the purposes it was collected for;
3. **Relevant** and **limited** to what is necessary for the purposes it is processed;
4. **Accurate** and kept **up to date**;
5. **Kept for no longer than is necessary** for the purposes for which it is processed; and
6. Processed in a manner that ensures **appropriate security** of the personal data.

The GDPR's broader "accountability" principle also requires that the School not only processes personal data in a fair and legal manner but that the School is also able to demonstrate that its processing is lawful. This involves, among other things:

- Keeping records of data processing activities, including by way of logs and policies.
- Documenting significant decisions and assessments about how the School uses personal data (including via formal DPIAs).
- Having an "audit trail" vis-à-vis data protection and privacy matters, including, for example:
    - When and how the School's Privacy Notices are updated.
    - When staff training was undertaken.
    - How and when any data protection consents were collected from individuals.
    - How personal data breaches were dealt with, whether or not reported (and to whom), etc.

Privacy by design
The School adopts a "privacy by design" approach to data protection to ensure that the School adheres to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help the School to achieve this, the School takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of Data Subjects when implementing data processes.

Data Protection Impact Assessments (DPIAs)
In order to achieve a privacy by design approach, the School conducts DPIAs for any new high-risk technologies or programmes being used by the School which could affect the processing of personal data. The School carries out DPIAs when required by the UK GDPR in the following circumstances:

- For the use of new technologies (programs, systems or processes) or changing technologies.
- For the use of automated processing.
- For large scale processing of Special Category Data.
- For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

DPIAs contain: -

- A description of the processing, its purposes and any legitimate interests used.
- Details of what types of data are shared.
- Steps taken by the third party and the school in order to protect data.
- An assessment of the necessity and proportionality of the processing in relation to its purpose.
- An assessment of the risk to individuals.
- The risk mitigation measures in place and demonstration of compliance.

Training
The School will ensure that staff and governors have undergone relevant and adequate data protection training to enable them to comply with data privacy laws. The School will provide training and appropriate guidance on a regular basis.

Audit
The School, through its DPO, will regularly test its data systems and processes in order to assess compliance. These are done through data audits which take place annually in order to review use of personal data.

LAWFUL GROUNDS FOR DATA PROCESSING

Under the UK GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, because the definition of what constitutes as consent has been tightened under UK GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the School to rely on another lawful ground where possible.

One of these alternative grounds is "legitimate interests", which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the School. It can be challenged by data subjects and also means the School is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in its Privacy Notice, as the UK GDPR requires.

Other lawful grounds include:

- Compliance with a legal obligation, including in connection with employment, engagement of services and diversity;
- Contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors;
- A narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

HEADLINE RESPONSIBILITIES FOR ALL STAFF

Record-keeping
It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the School if they believe that any personal data is inaccurate or untrue or if they are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues, pupils and their parents – in a way that is professional and appropriate.

Staff should be aware of the range of Data Subject Rights, whereby any individuals about whom they record information on school business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position for staff is to record every document or email in a form that they would be prepared to stand by should the person about whom it was recorded ask to see it.

The School is required to keep full and accurate records of its data processing activities. These records include:

- The name and contact details of the School.
- The name and contact details of the Data Protection Officer.
- Descriptions of the types of personal data used.
- Description of the Data Subjects.
- Details of the School's processing activities and purposes.
- Details of any third party recipients of the personal data.
- Where personal data is stored.
- Retention periods.
- Security measures in place.

Data handling
All staff have a responsibility to handle the personal data with which they come into contact fairly, lawfully, responsibly and securely and in accordance with all relevant School policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and IT security. Responsible processing also extends to the creation and generation of new personal data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

Avoiding, mitigating and reporting data breaches
One of the key obligations contained in the GDPR is on reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the School must keep a record of any personal data breaches, regardless of whether there is a need to notify the ICO. The Head of Legal, Risk and Assurance will report on data breaches to the Audit, Risk and Compliance Committee each Term.

If staff become aware of a personal data breach then they must notify the Data Protection Team by completing a data breach report via the Intranet homepage (under "Data Breach Reporting"). If staff are in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious, or it may be minor; and it may involve fault or not; but the School always needs to know about them to make a decision. The Head of Legal, Risk and Assurance, or any other member of the Data Protection Team, will be in contact with staff shortly after staff have submitted the breach report to clarify the extent of the breach and mitigations taken.

As stated above, the School may not need to treat the incident itself as a disciplinary matter. However, a failure to report could result in significant exposure for the School, and for those affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

Care and data security
More generally, all School staff are required and all contractors expected to remain mindful of the data protection principles (see above), and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue, but one that affects daily processes, such as filing and sending correspondence, notably hard copy documents. Data handlers should always consider what the most assured and secure means of delivery might be, and what the consequences would be of loss or unauthorised access.

The School expects all those with management / leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the School to Data Protection Team, and to identity the need for (and implement) regular staff training. Staff must attend any training required.

RIGHTS OF INDIVIDUALS

In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller (i.e.: the School). This is known as the "subject access right" (or the right to make "subject access requests"). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If a member of staff becomes aware of a subject access request (or indeed any communication from an individual about their personal data), the Head of Legal, Risk and Assurance must be informed as soon as possible either directly or by email to dataprotection@westminster.org.uk.

Requests from pupils will be processed in the same way as any other subject access request and information will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request. In general, the School will assume that pupils' consent to disclosure of their personal data to their parents (e.g.: for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare), unless, in the School's opinion, there is a good reason to do otherwise.

However, where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the School will maintain confidentiality unless, in the School's opinion, there is a good reason to do otherwise (e.g.: where the School believes disclosure will be in the best interests of the pupil or other pupils).

Individuals also have legal rights to:

- Require the School to correct the personal data held about them if it is inaccurate;
- Request the erasure of their personal data (in certain circumstances);
- Request the restriction of the School's data processing activities (in certain circumstances);
- Receive from the School the personal data held about them for the purpose of transmitting it in a commonly used format to another data controller;
- Object, on grounds relating to their particular situation, to any of the School's particular processing activities where the individual feels this has a disproportionate impact on them.

None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:

- Object to automated individual decision-making, including profiling (i.e.: where a significant decision is made about the individual without human intervention);
- Object to direct marketing;
- Withdraw one's consent where the School is relying on it for processing personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

In any event, however, if a member of staff receives a request from an individual who is purporting to exercise one or more of their data protection rights, they must tell the Head of Legal, Risk and Assurance or any other member of the Data Protection Team as soon as possible.

ENFORCEMENT
This Policy forms part of the terms and conditions of all employees' contracts of employment. A breach of the policy may be regarded as misconduct, leading to disciplinary action up to and including summary dismissal. It also applies to all members of the Governing Body and other officers of the School and breach of this Policy may result in appropriate action being taken by the School.

QUERIES AND COMPLAINTS
Any comments or queries on this Policy should be directed to Head of Legal, Risk and Assurance at dataprotection@westminster.org.uk or in writing using the following contact details:

Head of Legal, Risk and Assurance
Westminster School
17 Dean's Yard,
London
SW1P 3PB

If an individual believes that the School has not complied with this Policy or acted otherwise than in accordance with the DPA 2018, they should also notify the Head of Legal, Risk and Assurance.

Further information about data protection regulation and compliance can be found on the Information Commissioner's Office website: www.ico.org.uk

Below are details of the School's Data Protection Officer:

Data Protection Officer: Judicium Consulting Limited.
Address: 72 Cannon Street, London, EC4N 6AE.
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 option 1 then option 1 again.

ANNEX A

DATA SECURITY PRINCIPLES

- Access to personal data is provided to members of staff who require access to that personal data to perform their duties and responsibilities. As a result, different members of staff will have access to different categories of personal data depending upon their role.

- The security measures in place to protect data held electronically are set out in the Acceptable Use of Computer Network by Staff and Acceptable Use of Computer Network by Pupils Policies, which are reviewed regularly. All data on the Westminster networks is protected by anti-virus software that runs on servers and workstations, and is updated automatically. Data on the network is backed-up daily.

- Personal data held in manual files is only accessible by authorised individuals and, where of a confidential nature, is kept in locked filing cabinets when not in use.

- Paper-based copies of personal data (or other sensitive or confidential data) are disposed of in a secure manner, by shredding. Decommissioned IT equipment has data destruction procedures applied prior to its disposal.

- The physical security of the School premises is checked by the Security Department daily.

- The School ensures that, prior to the transfer of any personal data to a third party for processing, the third party has appropriate technical and organisational security measures governing the processing to be carried out.

- New staff are required to read and understand the Acceptable Use Policy as part of their induction.

- Any lapses in data security must be reported to the Director of Digital Strategy and Operations at the earliest opportunity.